ISO 42001 Annex C Assessment: 10-Step Process and Deliverables

Overview
ISO 42001 Annex C provides **informative guidance** on AI-related organizational objectives and risk sources to support AI risk management and impact assessments. While Annex C doesn't prescribe a specific assessment methodology, it serves as a foundation for establishing comprehensive AI governance frameworks.

10-Step Assessment Process

Step 1: Establish Assessment Scope and Context
Objective: Define the boundaries and context for the AI risk assessment using Annex C guidance.

Activities:
- Define which AI systems and organizational units are included
- Identify relevant stakeholders and interested parties
- Establish assessment timeline and resources
- Document internal and external context factors

Deliverables:
- Assessment scope statement
- Stakeholder mapping document
- Context analysis report

Step 2: Review and Select Organizational Objectives
Objective: Identify relevant AI-related organizational objectives from Annex C guidance.

Activities:
- Review Annex C organizational objectives (e.g., accountability, fairness, explainability, security)
- Select objectives applicable to your AI systems and organizational context
- Customize objectives to align with business strategy
- Define measurable success criteria for each objective

Deliverables:
- Selected organizational objectives matrix
- Customized objective definitions
- Success criteria documentation

Step 3: Identify and Catalog Risk Sources
Objective: Systematically identify AI-related risk sources using Annex C framework.

Activities:
- Review Annex C risk source categories
- Identify specific risk sources relevant to your AI systems

- Categorize risks by impact area (technical, ethical, operational, legal)
- Document risk source descriptions and potential impacts

Deliverables:
- Risk source inventory
- Risk categorization matrix
- Risk source impact analysis

Step 4: Conduct AI System Inventory and Classification
Objective: Document all AI systems and classify them according to risk levels and objectives.

Activities:
- Inventory all AI systems within scope
- Classify systems by type, purpose, and criticality
- Map systems to relevant organizational objectives
- Assess system lifecycle stage and maturity

Deliverables:
- AI system inventory
- System classification matrix
- Objective-to-system mapping document

Step 5: Perform Risk Assessment
Objective: Evaluate risks against organizational objectives using identified risk sources.

Activities:
- Assess likelihood and impact of identified risks
- Evaluate risks against each organizational objective
- Use risk matrices or scoring methodologies
- Consider cumulative and interdependent risks
- Document risk assessment rationale

Deliverables:
- Risk assessment report
- Risk register with scoring
- Risk heat map/matrix
- Assessment methodology documentation

Step 6: Conduct AI System Impact Assessment
Objective: Assess broader impacts of AI systems on individuals, groups, and society.

Activities:
- Evaluate impacts on different user groups and stakeholders
- Assess fairness, bias, and discrimination potential
- Consider environmental and societal impacts
- Analyze privacy and data protection implications
- Document impact assessment findings

Deliverables:
- AI system impact assessment report

- Stakeholder impact analysis
- Bias and fairness evaluation
- Privacy impact assessment

Step 7: Gap Analysis Against Objectives
Objective: Identify gaps between current state and desired organizational objectives.

Activities:
- Compare current AI governance practices against selected objectives
- Identify control and process gaps
- Assess capability and resource gaps
- Prioritize gaps based on risk and business importance

Deliverables:
- Gap analysis report
- Control gap matrix
- Prioritized improvement roadmap
- Resource requirement analysis

Step 8: Develop Risk Treatment Plans
Objective: Create actionable plans to address identified risks and gaps.

Activities:
- Define risk treatment strategies (avoid, mitigate, transfer, accept)
- Select appropriate controls from Annex A or develop custom controls
- Create implementation timelines and assign responsibilities
- Establish monitoring and review mechanisms

Deliverables:
- Risk treatment plan
- Control selection rationale
- Implementation roadmap
- Responsibility assignment matrix (RACI)

Step 9: Implementation and Monitoring Framework
Objective: Establish ongoing monitoring and measurement of objectives and risks.

Activities:
- Define key performance indicators (KPIs) for each objective
- Establish monitoring and measurement processes
- Create reporting mechanisms and frequency
- Implement continuous improvement processes

Deliverables:
- Monitoring and measurement plan
- KPI dashboard framework
- Reporting templates and schedules
- Continuous improvement procedures

Step 10: Documentation and Review

Objective: Complete comprehensive documentation and establish review cycles.

Activities:
- Compile comprehensive assessment documentation
- Conduct management review of findings and plans
- Establish periodic review and update cycles
- Create communication materials for stakeholders

Deliverables:
- Final assessment report
- Executive summary
- Management review minutes
- Communication plan and materials

Key Deliverables Summary

Primary Assessment Outputs:
1. **AI Governance Framework** - Comprehensive framework aligned with Annex C objectives
2. **Risk Management Plan** - Detailed risk treatment and monitoring plans
3. **Control Implementation Roadmap** - Prioritized action plan for control deployment
4. **Compliance Documentation** - Evidence of systematic AI risk management approach

Supporting Documentation:
- Assessment methodology and procedures
- Stakeholder engagement records
- Risk and impact assessment templates
- Monitoring and reporting frameworks
- Training and awareness materials

Integration with ISO 42001 Requirements

This Annex C assessment process directly supports:
- **Clause 6.1** - Actions to address risks and opportunities
- **Clause 6.2** - AI objectives and planning
- **Clause 8.2** - AI risk assessment
- **Clause 8.4** - AI system impact assessment
- **Clause 9.1** - Monitoring, measurement, analysis and evaluation

Best Practices

Cross-functional Involvement: Engage technical, legal, ethical, and business stakeholders throughout the process.

Iterative Approach: Treat this as an ongoing process rather than a one-time activity.

Documentation Standards: Maintain comprehensive records to support audit and certification requirements.

Continuous Improvement: Regularly update assessments as AI systems and regulatory landscape evolve.

Note: This process framework is based on the informative guidance provided in ISO 42001 Annex C and should be tailored to your organization's specific context, AI systems, and risk profile.